

# Number-theoretic expressions obtained through analogy between prime factorization and optical interferometry

Gabriel Seiden<sup>1</sup>

<sup>1</sup>*Department of Environmental Sciences and Energy Research,  
Weizmann Institute of Science, Rehovot 76100, Israel\**

Prime factorization is an outstanding problem in arithmetic, with important consequences in a variety of fields, most notably cryptography. Here we employ the intriguing analogy between prime factorization and optical interferometry in order to obtain, for the first time, analytic expressions for closely related functions, including the number of distinct prime factors.

PACS numbers: 02.10.De, 42.25.Hz

For millennia, people have been fascinated with the world of numbers and in particular with prime numbers. As early as 300 BC Euclid proved the infinitude of the primes and laid the foundation for the proof of the fundamental theorem of arithmetic. The last centuries have seen a surge in scientific activity focused on the primes and related mathematical themes, with leading mathematician such as Euler and Riemann greatly contributing to our current knowledge regarding the complexity of the distribution of primes. However, prime factorization of integers, especially that of large numbers, is still a formidable task. As a consequence, different applications in fields such as cryptography have been developed, which take advantage of the great difficulty of factoring large numbers (e.g., the RSA cryptosystem [1]).

During the last decades, physicists have contributed to the investigation of integer factorization as well as related mathematical topics, such as the Riemann hypothesis (see [2] and the references therein), through investigating the relationship with various physical systems. In particular, the intriguing relationship between quadratic Gauss sums and integer factorization has led to recent experimental realization of integer factorization through NMR and optical interference (see e.g., [3–7]).

In this Letter we explore the relationship between prime factorization and optical interference with the aim of obtaining novel analytic expressions for number-theoretic functions directly related to prime factorization. Our study, which is based on the relationship between the multiple-slit interference experiment and the occurrence of the primes, exhibits the potential of physical analogy not only in realizing a mathematical enigma experimentally, but also contributing to the theoretical endeavor to unravel the enigma.

The fundamental theorem of arithmetic states that any positive integer  $n$  can be decomposed into prime numbers in a unique manner, that is:

n	2	3	5	7	11	13	17	19	23	$\omega(n)$
1	0	0	0	0	0	0	0	0	0	0
2	1	0	0	0	0	0	0	0	0	1
3	0	1	0	0	0	0	0	0	0	1
4	2	0	0	0	0	0	0	0	0	1
5	0	0	1	0	0	0	0	0	0	1
6	1	1	0	0	0	0	0	0	0	2
7	0	0	0	1	0	0	0	0	0	1
8	3	0	0	0	0	0	0	0	0	1
9	0	2	0	0	0	0	0	0	0	1
10	1	0	1	0	0	0	0	0	0	2
11	0	0	0	0	1	0	0	0	0	1
12	2	1	0	0	0	0	0	0	0	2
13	0	0	0	0	0	1	0	0	0	1
14	1	0	0	1	0	0	0	0	0	2
15	0	1	1	0	0	0	0	0	0	2
16	4	0	0	0	0	0	0	0	0	1
17	0	0	0	0	0	0	1	0	0	1
18	1	2	0	0	0	0	0	0	0	2
19	0	0	0	0	0	0	0	1	0	1
20	2	0	1	0	0	0	0	0	0	2
21	0	1	0	1	0	0	0	0	0	2
22	1	0	0	0	1	0	0	0	0	2
23	0	0	0	0	0	0	0	0	1	1
24	3	1	0	0	0	0	0	0	0	2
25	0	0	2	0	0	0	0	0	0	1

TABLE I: Prime factorization of the first twenty-five positive integers. The rightmost column presents the corresponding number of distinct prime factors.

$$n = \prod_{i=1}^{\omega(n)} p_i^{\alpha_{p_i}(n)}, \quad (1)$$

where  $\omega(n)$  is the number of distinct primes function,  $p_i$  is the  $i^{\text{th}}$  prime and  $\alpha_{p_i}(n)$  is the corresponding power. Table I depicts the integer decomposition into primes of the first twenty-five integers. From the table one can deduce three features of prime factorization. First, one notes that each prime appears periodically as  $n$  increases, with a period equal to the corresponding prime. This is





the functional dependency pertaining to the occurrence of the corresponding prime in the factorization of the integers. We then examined the partial sum  $\omega_m(n)$ , pertaining to the intensity field of  $m$  sets, each consisting of a prime number of narrow slits, and elaborated on its connection with the sieve of Eratosthenes. An analytic expression for the number of distinct prime factors  $\omega(n)$  was then derived through taking the limit of infinite sets of slits. Finally, we also obtained analytic expressions for the functions  $\alpha_p(n)$  and  $\Omega(n)$ , which together with  $\omega(n)$  completely define prime factorization.

---

\* Electronic address: gabriel.seiden@weizmann.ac.il

- [1] R. L. Rivest, A. Shamir, and L. Adleman, *Comm. ACM* **21**, 120 (1978)
- [2] D. Schumayer and D. A. W. Hutchinson, *Rev. Mod.*

- Phys.* **83**, 307 (2011)
- [3] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, *Nature* **414**, 883 (2001)
- [4] M. Mehring, K. Müller, I. Sh. Averbukh, W. Merkel, and W. P. Schleich, *Phys. Rev. Lett.* **98**, 120502 (2007)
- [5] D. Bigourd, B. Chatel, W. P. Schleich, and B. Girard, *Phys. Rev. Lett.* **100**, 030202 (2008)
- [6] V. Tamma, H. Zhang, X. He, A. Garuccio, W. P. Schleich, and Y. Shih, *Phys. Rev. A* **83**, 020304(R) (2011)
- [7] W. Merkel, S. Wölk, W. P. Schleich, I. Sh. Averbukh, B. Girard, and G. G. Paulus, *New J. Phys.* **13**, 103008 (2011)
- [8] S. G. Lipson, H. Lipson, and D. S. Tannhauser, *Optical Physics* (Cambridge University Press, 1995)
- [9] G. H. Hardy and S. Ramanujan, *Quart. J. Math.* **48**, 76 (1917)
- [10] P. Erdős and M. Kac, *Am. J. Math.* **62**, 738 (1940)
- [11] G. H. Hardy and E. M. Wright, *An Introduction to the theory of numbers* (Oxford University Press, 1979)